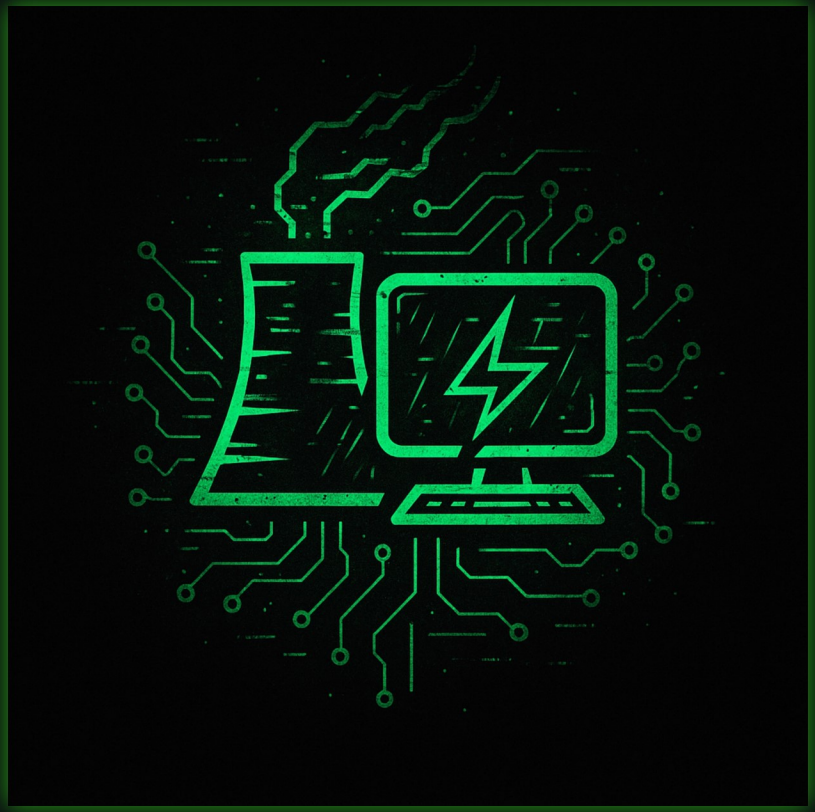

Nikolaos Kranidiotis – OSEC.GR

Power Plant Cybersecurity & Forensics Cheat Sheet

1) Safety & Quick Triage (OT-aware)

- **Safety & stability first.** Coordinate with operations. No action that can alter process state without explicit approval.
- **Start passive.** Use SPAN/TAP for traffic observation and collect logs. *No active scans* until risk-assessed and authorized.
- **Protect critical loops.** Do not reboot/stop HMIs, PLCs, SIS, turbine/governor or excitation controllers while controlling the process.
- **Logical isolation over power-off.** Quarantine hosts via switch/VLAN if needed; keep controllers/HMIs running when safe.
- **Regulatory awareness.** Know reportable thresholds (e.g., NERC CIP in North America) and internal escalation paths.
- **Record time sources.** Note UTC vs local plant time, GPS/NTP status, and any offsets/drift. Log actions/observations in real time.

2) Architecture & Asset Classes

- **Zones/Levels.** Purdue-style: L0/1 field (sensors, actuators), L2 control (PLCs/RTUs, HMIs, SCADA), L3 site ops (EWS, historians, AD), L3.5 DMZ, L4 IT.
- **Core systems.** DCS (e.g., Siemens PCS7, Emerson Ovation), HMIs, EWS, Historians (e.g., OSIsoft PI), PLCs/RTUs, IEDs (SEL/ABB/GE relays), SIS.
- **Boundary controls.** Industrial firewalls, data diodes (one-way), jump hosts. Prefer one-way telemetry, controlled interactive access.
- **Time sync.** GPS/NTP/PTP/IRIG-B for relays/IEDs. Accurate time underpins forensics & protection coordination.
- **Field buses.** Legacy serial (Modbus RTU, Profibus) via gateways; Ethernet-based I/O (PROFINET, EtherNet/IP). Document conduits & trust.

3) ICS/OT Protocols & Ports (quick ref)

Protocol	Port	Use	Notes
Modbus/TCP	502/tcp	Classic PLC/RTU telemetry & control	No auth/enc by design; reads/writes (FC 1,3 vs 5,6,15,16). Limit to known pairs.
DNP3 (IEEE 1815)	20000/ tcp,udp	Electric SCADA master↔outstation	Default cleartext; DNP3-SA/TLS optional but not ubiquitous. Sequence numbers aid replay detection.
IEC 60870-5-104	2404/tcp	International telecontrol (SCADA)	Usually cleartext; IEC 62351 for TLS. Widely used in EU/Asia.
IEC 61850 MMS	102/tcp	IED config/SCADA over MMS	TLS via IEC 62351-4 possible; often open (clear). Used with GOOSE/SV at L2.
IEC 61850 GOOSE	L2 0x88B8	Substation events/trips (~ms)	Ethernet multicast; no crypto. Requires local TAP to capture.
IEC 61850 SV	L2 0x88BA	Sampled analog values	High-rate multicast; PTP timing. Capture only via TAP.
OPC UA	4840/tcp	Secure data exchange	Supports cert-based auth/enc. Verify security policy ≠ None.

Capture (passive): `tcpdump -i <if> '(tcp port 502 or 20000 or 2404 or 102 or 4840)' -w ot.pcap`

4) Threat Landscape (concise)

- **APT & sabotage.** Grid/plant targeting (e.g., controller/relay misuse, OT malware). Long dwell, precise objectives.
- **Ransomware spillover.** IT compromise forcing OT shutdown; occasional lateral movement into HMIs/servers.
- **Vendor/remote access risk.** Stolen creds, poorly secured VPNs/jump hosts; supply-chain trojans.
- **Insider/contractor.** Misuse of engineering tools, logic/setting changes, USB introduction.
- **General malware.** Legacy Windows hosts in OT impacted by worms → HMI instability/network noise.

5) Frequent Weaknesses

- Flat networks; weak or no zoning/whitelisting.
- Legacy OS & unpatched firmware with compensating controls missing.
- Default/shared accounts; no MFA; weak role separation.
- Insecure-by-design protocols reachable from IT or internet.
- Limited logging/monitoring; short device log retention.
- Poor USB/portable device governance; weak physical/port security.

6) Forensic Readiness & Evidence Sources

- **Centralize logs.** Syslog/Windows EVTX forwarders into an OT collector (one-way to IT if needed).
- **Historian.** Export CSVs for incident window; check gaps/backfills vs events/alarms.
- **Backups & baselines.** Secure repositories of PLC logic, relay settings, HMI/EWS projects; include hashes and version notes.
- **Device event stores.** PLC diagnostics, relay SOE/fault records, DCS alarm journals, firewall/VPN logs.
- **Time hygiene.** NTP/GPS/PTP across plant; periodically verify offsets & drift.
- **People/process.** Operator logs, badge access, maintenance tickets—correlate with technical data.

7) Live Response (Do-No-Harm)

- Prefer **passive collection** (SPAN/TAP, log exports). Avoid interaction with controllers while in control.
- Isolate **logically** first; keep power/process continuity. Defer reboots until evidence is acquired & operations approves.
- Capture **volatile data** on Windows HMIs/servers using vetted tools; for PLCs, retrieve diagnostic buffers via read-only vendor tools.
- Coordinate **mode changes** (e.g., PROGRAM/STOP) with engineering on a bench/testbed where possible.
- Document **clock & timezone** per asset; photo screens if needed.
- Preserve suspicious binaries/logic to offline media; analyze in lab/sandbox, not on production hosts.

8) Indicators & What to Hunt

- Off-hours PLC/DCS downloads; unexpected firmware updates; controller mode toggles.
- Protocol misuse: Modbus writes (FC 5/6/15/16), DNP3 select/operate, IEC-104 C_SC/ C_DC commands atypical for baseline.
- Relay/IED setting drift vs baseline; lockouts disabled; protection group changes.
- Historian anomalies: gaps/backfills, sudden flatlines, suppressed or flood alarms.
- New peers/flows IT↔OT; unexpected protocols (FTP/SMB/HTTP) in control LAN.
- Access anomalies: VPN/jump host logins at odd times; new admin accounts; AD group changes in OT domain.

9) Remote Access & Vendor Channels

- Inventory all vendor paths: VPNs, modems, cloud brokers, jump hosts, data diodes (list owner, purpose, hours).
- Enforce JIT access, MFA, source IP allowlists; sessions **only via DMZ jump hosts** with full auditing/screen record.
- Prefer read-only one-way data export for routine needs; minimize interactive remote support.
- Disable dormant/always-on tunnels; remove legacy dial-up where possible.
- Log & review every remote session; tie actions to individuals (no shared vendor accounts).

10) Assessment Method (OT-aware)

- Define ROE + MOC: what's allowed, windows, rollback plans, safety breakers.
- Start passive discovery (maps/pcaps/configs) → only then controlled active checks in maintenance windows.
- Lab-first: test scans/tools on identical hardware/firmware. Throttle, read-only queries.
- Integrity checks: compare controller logic/settings/firmware hashes to gold images.
- Exercises: tabletop & bench simulations for IR (e.g., HMI malware, comms loss, bad logic injects).
- Readiness review: logging, retention, backups, spares, vendor SLAs, escalation lists.

11) Timeline & Correlation

- Normalize to UTC; record per-asset offset. Note DST/state.
- Correlate network logs, EVTX/syslog, historian trends, device SOE, operator notes on one axis.
- Use tooling (Plaso/Timesketch) or spreadsheet with categories (network/user/device/physical) to see cause→effect.
- Cross-verify key moments (e.g., remote login → EWS download → process deviation).
- Watch for anti-forensics: log gaps, time jumps, wiped audit trails.
- Maintain chain-of-custody for all artifacts and exported evidence.

12) Containment & Recovery (non-disruptive)

- Prefer **network containment** (ACL/VLAN) over device power-off.
- Fail over to redundant HMI/SCADA if available; clean affected host offline.
- Engage OEMs/engineering for safe firmware reloads/config restores.
- Use known-good backups; validate with checksums; keep compromised units for forensics if possible.
- Stage back to normal: reduced load/manual mode with heightened monitoring first.
- Communicate with grid/regs as required; document decisions/risks/tradeoffs.

13) Hardening & Monitoring

- Segment per ISA/IEC 62443 zones/conduits; default-deny rulesets.
- Harden endpoints: least privilege, app whitelisting, disable unused services, secure boot where supported.
- Strong auth: unique accounts, RBAC, PAM for elevated access, MFA for remote/jump/critical ops.
- USB controls: approved media only; dedicated scanning station; controlled maintenance laptops.
- Patch on cadence with outage planning; if not patchable, add compensating controls and risk register.
- ICS-aware monitoring: protocol IDS/behavioral alerts (write ops, mode changes, firmware upload attempts).
- Integrity verification: FIM on Windows; controller logic checksum/signature checks against gold.
- Training & SOPs: include cyber in drills; vendor onboarding with security requirements.

14) Tools & Parsers

Purpose	Examples	Notes
Packet capture/ analysis	tcpdump, Wireshark, Zeek (ICS parsers)	SPAN/TAP only. Decode Modbus/DNP3/IEC 104/MMS/OPC UA; hunt writes/operates.
Passive discovery	GRASSMARLIN, Rumble (runZero)	Inventory with minimal risk; prefer pcap-driven mapping where possible.
Logs/SIEM	ELK/OpenSearch, Splunk	Aggregate EVTX/syslog/OT firewall; alert on controller mode, new peers, failed logins.
Timeline	Plaso (log2timeline), Timesketch	Merge multi-source events; pivot by host/user/action.
Vendor tools (read-only)	Siemens TIA/Step7; Schneider EcoStruxure; GE ToolboxST; ABB PCM600; SEL AcSELerator	Pull diagnostics, SOE, configs; compare to baselines. *Use read-only where possible.*
Protocol tooling	OpenDNP3, modbus-cli, MMS libs	Bench/tabletop testing & parsers; not for production networks.

15) Evidence Examples & Paths (vendor- & version-specific)

- **Windows EVTX (HMI/Server):** `C:\Windows\System32\Winevt\Logs\*.evtx` → export with `wevtutil epl` (read-only).
- **Historian (example OSIsoft PI, version-specific):** archives under `C:\Program Files\PI\Data\`; export trends to CSV via PI tools.
- **HMI/SCADA journals (example vendor-specific):** CSV/XML event/alarm logs (e.g., `D:\<DCS>\Events\*.csv`).
- **Siemens S7/PCS7 (example):** Project dirs and download history via TIA Portal; PLC diagnostic buffer export (tool-based).
- **GE Mark VIe (example):** ToolboxST audit trail & SOE exports; controller firmware/version summaries (tool-based).
- **ABB Relays (example):** PCM600 retrieve settings/SOE; export COMTRADE `.CFG/.DAT` for faults.
- **SEL Relays (example):** AcSELerator export event reports/SER (Sequence of Events); COMTRADE files like `EVENT####.CFG/.DAT/.HDR/.INF`.
- **Firewalls/VPN:** Export CSV/syslog from OT firewalls/VPN concentrators (mgmt UI or syslog server).
- **Network PCAP:** From span/TAP recorders or sensors; include L2 captures for GOOSE/SV where applicable.

16) Governance & Standards (for reports)

- **NIST SP 800-82:** ICS security guidance (US).
- **ISA/IEC 62443:** Global framework (zones/conduits, SLs, component/system reqs).
- **NERC CIP (North America):** Mandatory for BES entities (e.g., CIP-007, CIP-008 incident response).
- **ISO/IEC 27019:** Energy-sector adaptation of ISO/IEC 27002 controls.
- **IEC 62351:** Security for power comms (adds TLS/auth to 60870-5, 61850).
- **MITRE ATT&CK for ICS:** Technique mapping for OT adversary behavior.
- **Regional guidance:** e.g., EU NIS/NIS2, UK NCSC ICS guidance, national CERT advisories.

17) Quick Command & Filter Snippets

- **tcpdump (passive capture):** `tcpdump -i eth0 -s0 -w ot.pcap 'tcp port 502 or 20000 or 2404 or 102 or 4840'`
- **GOOSE/SV (L2):** `tcpdump -i eth0 'ether proto 0x88B8' -w goose.pcap` / `tcpdump -i eth0 'ether proto 0x88BA' -w sv.pcap`
- **tshark display filters:** Modbus writes `-Y "modbus.func_code in {5,6,15,16}"` · DNP3 operates `-Y "dnp3.func_code == 0x05"` · IEC104 commands `-Y "iec60870_5_asdu.typeid in {45,46,58,59}"` · MMS `-Y "mms"` · OPC UA `-Y "opcua"`
- **Windows EVTX export (read-only):** `wevtutil epl Security D:\ir\Security.evtx` · `wevtutil epl System D:\ir\System.evtx`
- **Windows quick triage (text):** `tasklist /V > D:\ir\tasks.txt` · `netstat -ano > D:\ir\netstat.txt` · `wmic qfe > D:\ir\patches.txt`
- **Linux logs/process:** `journalctl --since "2025-08-01" > /tmp/journal.txt` · `ps -ef > /tmp/ps.txt` · `ss -tulpn > /tmp/sockets.txt`
- **Zeek ICS logs (if enabled):** review `modbus.log`, `dnp3.log`, `iec104.log`, `mms.log` for command summaries.
- **Historian export (example, vendor-specific):** Use vendor read-only export to CSV around incident window; do not write back or reprocess live tags.